UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,928	03/31/2000	Ulhas S Warrier	10559-148001/P7973	2224

20985 7590 12/13/2005

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER
TRAN, ELLEN C

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/539,928	**Applicant(s)** WARRIER ET AL.
	Examiner Ellen C. Tran	**Art Unit** 2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6-23 and 25-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,6-23 and 25-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: amendment filed on 16 September 2005, with acknowledgement of original filing date of 31 March 2000 with a declaration swearing back to a date of conception prior to 12 January 2000.

2. Claims 1, 2, 3, 6-23, 25-34 are currently pending in this application. Claims 1, 9, 17, 21, and 30 are independent claims. Claims 4, 5, and 24 have been previously withdrawn.

Response to Arguments

3. Applicant's arguments filed 16 September 2005 have been fully considered, however they are moot due to new grounds of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1, 2, 3, 6-23, 25-34,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund U.S. Patent No. 5,987,611 (hereinafter '611).

As to independent claim 1, "A method of managing a network session comprising delivering security policies from a server to a remote system that has predetermined configuration information" is taught in '611 col. 21, line 47 through col. 22, line 30;

"and allows running at least one application program" is shown in '611 col. 4, lines 5-29;

"regulating activities in the system based on both of the security policies and a context of said at least one application program including at least a state of running of said at least one application program" is disclosed in '611 col. 4, lines 51-63;

the following is not taught in '611 **"establishing a secure virtual private network connection between the server and the system"** however '611 teaches "The centralized supervisor application is installed on a computer on the LAN that can be reached from all workstations that need access to the Internet; this is typically (although not necessarily) a server computer ... The communication between the client-based filter and the centralized supervisor application, as well as between the supervisor application and the firewall, employs encryption to ensure secure communication and avoid any possible attack on that level" in col. 5, lines 6-20.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a computer environment with methods of monitoring access taught in '611 to include a means to adapt policies or filters for a Virtual Private Network. One of ordinary skill in the art would have been motivated to perform such a modification because encrypted communications between a server and a client is a VPN. In addition most VPNs use communication with an authentication server to allow a client to access the network see col. 21, line 65 through col. 22, line 15 "When a user dials into a POP (e.g., using a protocol such as SLIP), the POP server in return contacts the central ISP authentication server either via the Internet or a dedicated line".

As to dependent claims 2, "wherein said regulating the activities comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria that are conditioned on said running state" is taught in '611 col. 4, lines 5-39.

As to dependent claim 3, "wherein the rejection criteria include the predetermined configuration information" is shown in '611 col. 4, lines 5-39.

As to dependent claims 6, "wherein regulating the activities comprises: providing a session layer adapted to reject unauthorized data packets based on context information; and providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies" is disclosed in '611 col. 16, lines 8-29.

As to dependent claim 7, "further comprising updating the set of policies" is taught in '611 col. 27, lines 17-21.

As to dependent claim 8, "further comprising: detecting data packets from the regulated activities; and rejecting the data packets from the regulated activities" is shown in '611 col. 27, lines 9-16.

As to independent claim 9, this claim is directed to a computer-readable medium of the method of claim 1 and is rejected along similar rationale.

As to dependent claims 10, 11, 12, 14, 15, and 16, these claims contain substantially similar subject matter as claims 2, 3, 6, 7, and 8 above; therefore they are rejected along the same rationale.

As to dependent claim 13, "wherein the rejection criteria includes the set of policies" is taught in '611 col. 4, lines 5-28.

As to independent claim 17, this claim is directed to the system of the method of claim 1 and is rejected along similar rationale.

As to dependent claim 18, "further comprising a network stack" is shown in '611 col. 4, lines 33-39.

As to dependent claim 19, "wherein the network stack comprises: a policy engine connected to the first device" is disclosed in '611 col. 3, lines 60-65 "At a general level, the present invention provides a system comprising one or more access management applications that set access rules for the entire LAN for one or more workgroups or individual users" (Note the police engine is interpreted to have the same meaning as 'management applications';

"a policy store connected to the policy engine" is taught in '611 col. 4, lines 5-8 "The access management application is employed by the LAN administrator, workgroup administrator, and/or LAN user to maintain a database of the access rules for the workstations being administrated" (Note the policy store is interpreted to have the same meaning as the 'database of the access rules');

"a socket interceptor connected to the policy engine" is shown in '611 col. 4, lines 29-64 " The client-based filter application, which in a preferred embodiment performs all of the monitoring, logging, and filtering work, is responsible for intercepting process loading and unloading. Other responsibilities include keeping a list of currently active processes; intercepting certain keyboard, mouse and other interactive user activities in order to determine which process is actively used; intercepting and interpreting all TCP/IP communication and build a comprehensive representation of these TCP/IP activities; and intercepting certain file activity and assign them to the originating process" (Note the client-based filter is interpreted to have the same meaning as 'socket interceptor'; also note, the client-side filter is controlled by the centralized authority see col. 3, lines 55-59);

"and a packet guard connected to the policy engine" is disclosed in '611 col. 3, line 67 through col. 4, lines 4 "Typically, the system includes (optionally) a firewall or similar application, which works together with the supervisor application in order to block all clients that have not been verified by the supervisor application" (Note the packet guard is interpreted to have the same meaning as the 'firewall or similar application').

As to dependent claim 20, "the first device further comprising instruction to monitor the system for the intervening process" is taught in '611 col. 4, lines 29-39.

As to independent claim 21, "A network stack comprising: a policy engine a policy store adapted to interact with the policy engine and store a set of policies from the policy engine; a socket interceptor coupled to the policy engine; a packet guard coupled to the policy engine; use the packet guard to filter unauthorized activities received from the network interface" is taught in '611 col. 3, line 55 through col. 4, line 64;

"use the packet guard to filter the data packets from unauthorized users and applications based on the context information received by the socket interceptor" is shown in '611 col. 16, lines 8-29;

"and use the packet guard to filter data packets based on the policies and provide the packet guard with context information about the unauthorized users and applications including at least information about a running state of the application" is disclosed in '611 col. 4, lines 5-39 and col. 9, lines 20-63;

"a configurable management process adapted to reconfigure the network stack and having instructions to: receive policies in the policy engine from the policy server" is taught in '611 col. 27, lines 17-21;

"use the socket interceptor to detect and reject data packets from unauthorized users and applications and provide the packet guard with context information about the unauthorized users and applications including at least information about a running state of the application" is disclosed in '611 col. 4, lines 51-63.

As to dependent claim 22, "The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard" is shown in '611 col. 21, lines 21-46.

As to dependent claim 23, "The network stack of claim 21 further comprising an interface to a network adapted to connect the network stack to the network, wherein the network has a policy server" is disclosed in '611 col. 22, lines 7-41.

As to dependent claim 25, "wherein said remote system includes a network stack, and wherein said regulating activities comprises reconfiguring the network stack to control filtering of network packets, based on said policies and said running state" is taught in '611 col. 27, lines 17-21.

As to dependent claim 26, "wherein said policies include information about authorized kinds of information when certain applications are running, and said regulating activities comprises determining if a specified application is running, allowing a specified kind of network packet to pass only when said specified application is running, and blocking said specified kind of network packet from passing when said specified application is not running" is taught in '611 col. 9, lines 20-63 and col. 16, lines 8-29.

As to dependent claim 27, "wherein said specified application is a word processing program, and said kind of network packet is word processing data" is shown in '611 col. 7, lines 18-25.

As to dependent claims 28 and 29, these claims are substantially similar to claim 26 above and are rejected along the same rationale.

As to independent claim 30, "A method, comprising: establishing a virtual private network (VPN) session between a primary computing system and a remote computing system" is taught in '611 col. 5, lines 6-20;

"includes a security policy engine, and wherein the primary computing system includes a security policy engine" is shown in '611 col. 3, lines 60-65;

"and wherein the remote computing system includes a network stack" is disclosed in '611 col. 21, lines 47-53;

"transmitting information indicative of security parameters from the primary computing system to the remote computing system using the security policy engine configuring the network stack based on the information indicative of security parameters" is taught in '611 col. 21, line 47 through col. 22, line 30;

"subsequently running a particular application program on the remote computing system; selecting information indicative of updated security parameters based on a running state of the particular application program and dynamically reconfiguring the network stack based on the information indicative of the updated security parameters" is shown in '611 col. 27, lines 17-36.

As to dependent claim 31, **"wherein the primary computing system is a corporate local area network (LAN)"** is disclosed in '611 col. 1, lines 51-67.

As to dependent claim 32 **"wherein the remote primary computing system is a remote home network"** is taught in '611 col. 1, lines 51-67.

As to dependent claim 33, **"wherein the particular application program is a word processing program"** is shown in '611 col. 7, lines 18-25;

"and wherein when the running state of the work processing program indicates that the word processing program is not running" is disclosed in '611 col. 13, lines 26-31;

"the information indicative of security parameters causes the remote computing system to block word processing packets received at the remote computing system" is disclosed in '611 col. 4, lines 51-67.

As to dependent claim 34, **"wherein the particular application program is a word processing program"** is shown in '611 col. 7, lines 18-25;

"and wherein when the running state of the word processing program indicates that the word processing program is running" is disclosed in '611 col. 13, lines 26-31;

"the information indicative of updated security parameters causes the remote computing system to not block word processing packets received at the remote computing system" is disclosed in '611 col. 4, lines 51-67 and col. 27, lines 9-16.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
11 December 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100